Remarks

No claims have been amended. Claims 1 and 9-18 are pending in this application.

Claim 1 stands rejected under 35 U.S.C. §102(e) as being anticipated by Kara (U.S. Patent No. 5,822,739). The Office Action, in response to Applicants previous arguments, contends that Kara discloses the use of a digital signature to sign a transaction record and storing the signed transaction record in a database. Reconsideration is respectfully requested.

The present invention is directed to a virtual postage metering system in which a host of personal computers (PC) are coupled to a server located at a data center. The host PC's do not have any Postage Storage Devices (PSD) coupled thereto; instead, all PSD functions are performed at the data center. The PSD is a secure processor-based accounting device that dispenses and accounts for postal value stored therein. The host PCs must connect with the data center to process transactions such as postage dispensing, meter registration or meter refills. Transactions are requested by the host PC and sent to the data center for remote processing. The transactions are processed centrally at the data center and the results are returned to the host PC. Accounting for funds and transaction processing are centralized at the data center. (Specification, page 4).

Although the data center may be a secure facility, there remain certain inherent security issues since the accounting and token generation functions do not occur in a secure device local to the postage meter. For example, data stored at the data center is accessible to data center personnel and, therefore, at a minimum, subject to at least inadvertent modification by such personnel. Any unauthorized changes to the user and meter data stored at the data center compromises the integrity of the virtual postage metering system. (Specification, page 5). The present invention alleviates these types of security issues by providing a virtual postage metering system in which the transaction records are signed with a digital signature and the signed transaction records are stored at the data center. Thus, if the information contained within the transaction record has been altered, the digital signature will not verify, thereby indicating that the information has been altered. Thus, the signed record is unalterable and the signature cannot be repudiated.

In view of the above, claim 1 is directed to a method for evidencing postage that comprises "generating a digital token . . . including encrypted information for the mailpiece . . . creating a transaction record . . . including the digital token and the postal information; signing the transaction record" and "storing the transaction record in a database at the data center."

The Office Action contends that Kara discloses signing a transaction record and storing the transaction record in a database at Col. 14, lines 12-36 and Col. 4, lines 37-50. Applicants respectfully disagree and respectfully request the Examiner to fully consider the following.

Col. 14, lines 12-38 of Kara state:

> Upon determination of proper funding, the Meter program increments a record of the amount of postage credit transmitted for later compensation to the Postal Authority. Alternatively, the Meter program deducts the amount of postage to be used by the postage indicia from a postage credit available at PC 10 (step 306). The Meter program may itself be provided with postage credit through such means as authorization by an official postal service, direct connection to a postal service office, or portable electronic postage credit. The details of the provision of postage credit to the Meter program is not shown, but may be, for example, the system shown in above referenced and incorporated U.S. Pat. No. 5,510,992.
>
> The Meter program may check the destination address included in the demand to verify that it is a proper address if desired. Address checking is accomplished by comparing the destination address to a database of addresses stored, for example, on disk drive 13 within PC 10.
>
> The Meter program utilizes information contained within the demand to generate a data packet representing the desired postage indicia (step 307). The data packet includes information required of a valid postage indicia by a postal service. Such information may include the date of posting, the amount of the postage, a unique transaction identifier, and identification of the metering device. The information may also include

> data to be printed with the postage indicia, such as the sender's return address, at the user's preference.

Col. 4, lines 37-50 of Kara state:

> In the preferred embodiment, the Demand program provides security at the demand site to prevent unauthorized utilization of the postage metering system. The appropriate level of security for any installation of the Demand program can be chosen by a principal at each location, thereby providing a distributed security system. Distributed security provides the ability for individual users of the postage metering system to select a level of security appropriate to prevent postal theft in their environment. Such distributed security does not increase the risk of postage loss at the remote meter as, regardless of the level of security chosen at the demand site, verification is performed by the Meter program to ensure each demand is valid and properly funded.

Note first that there is nothing in either of these passages that relates to signing a transaction record and storing the transaction record in a database as is recited in claim 1, nor has the Office Action provided any specific reference to where these features are allegedly disclosed. The Office Action contends that a "unique transaction identifier" is equivalent to signing a transaction. This is simply not true. The unique transaction identifier in Kara is merely an identifier of the transaction, such as, for example, a serial number or the like. Thus, the information contained within the transaction record can be altered or changed and the "unique transaction identifier" can remain the same. Thus, there is no way of determining if the information contained within the transaction record has been altered. The "unique transaction identifier" does not provide any type of protection against such alteration, nor does it provide any type of authentication of the author. A digital signature, in contrast, authenticates and protects the integrity of the information in the transaction record. If the information contained within the transaction record has been altered, the digital signature will not verify, thereby indicating that the information has been altered. Thus, the signed record is unalterable and the signature cannot be repudiated. These attributes are not present in a "unique transaction identifier," as there is no resemblance between a unique transaction identifier and a digital signature.

Col. 4, lines 37-50, is directed to providing security at the demand site to prevent unauthorized use of the postage metering system. In Kara, a demand program is stored on first processor-based system (PC) located within a business' office or an individual's home. The demand program accepts information from a user and makes a demand for postage to a remote postage meter, itself a second processor-based system in the form of a PC, that is located at a postage provider's office or other central source. The second PC stores a meter program that verifies postage demands and electronically transmits the desired postage indicia to the first PC in the form of a data packet. (Col. 3, line 55 to Col. 4, line 4). Thus, the security at the demand site is designed to limit access to the demand program. For example, as illustrated in Fig. 2 of Kara, at step 201 upon activation of the demand program, the user is asked for, and the process accepts, a user password. At step 202, the demand program determines if the accepted password is valid. If the password is not valid, the process returns to step 201, thus preventing unauthorized access to postage. (Col. 7, lines 47-55). This is in no way related to creating a transaction record, signing the transaction record, and storing the transaction record in a database at a data center as is recited in claim 1.

Furthermore, in Kara, a meter program is used to generate a data packet that is a digital representation or image of the postage indicia to be ultimately printed by the demanding site. The data packet includes information required of a valid postage indicia by a postal service. (Col. 14, lines 30-41). Thus, the data packet is sent to the demanding site for use in printing the indicia. Specifically, at step 308 of Fig. 3, the data packet generated from the received demand is transmitted via the data communications link to the demand site. (Col. 15, lines 1-3). There is no disclosure, teaching or suggestion in Kara of creating a transaction record, signing the transaction record, and storing the signed transaction record in a database at the data center as is recited in claim 1.

For at least the above reasons, Applicants respectfully submit that claim 1 is allowable over the prior art of record.

Claims 9-18 stand rejected under 35 U.S.C. §102(e) as being anticipated by, or, in the alternative, under 35 U.S.C. § 103(a) as obvious over, Whitehouse (U.S. Patent No. 6,005,945). Reconsideration is respectfully requested.

Claim 9 is directed to a system for dispensing postage that includes a data center, the data center comprising a "storage device," a "first cryptographic module" that includes a "first key to decrypt a user authentication key included in the user account, the user authentication key being used to authenticate the user; and a second cryptographic module . . . including a second key to decrypt a token key included the meter account, the token key used to generate a digital token, the second cryptographic module further including a third key used to sign a transaction record associated with generating the digital token, the signed transaction record being stored in the storage device."

The Office Action contends that Col. 8, lines 37-41 and Col. 14., lines 26-48 of Whitehouse disclose signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center. Applicants respectfully disagree and respectfully request the Examiner to fully consider the following.

Col. 8, lines 30-53, of Whitehouse state:

> Local memory 154, which will typically include both random access memory and non-volatile disk storage, preferably stores a set of postage dispensing procedures 160, including:
>
> a postage indicium request validation procedure 161 for validating requests from end user computers for postal indicia;
>
> message encryption and decryption procedures 162;
>
> encryption keys 164 needed to generate the digital signatures in postal indicia, and keys for secure communications with the postal authority computer system 180;

> a ZIP+4 or ZIP+4+2 procedure 166 for generating a ZIP+4 or ZIP+4+2 value for each destination address specified in a postage request message received from any of the customer PCS;
>
> an indicium generation procedure 168 for generating a sequence of bits representing a postage indicia corresponding to a destination address specified by a customer PC, including a procedure for digitally signing each postage indicium; and
>
> a communication procedure 170 for handling communications with the customer PCS 104.

While the above passage discusses the use of encryption keys to generate digital signatures in postage indicia, there is no disclosure, teaching or suggestion of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Col. 14, lines 25-56, state:

> The integrity of the balance update transaction depends upon a coordinated encryption/decryption between the funding entity (typically a postage meter vendor) and the end user. For conventional electronic meters, the encryption is based on a complex formula involving the internal meter ID, the amount of postage required, the descending and ascending registers in the meter, the date and other variables. Security in this transaction is absolutely critical because the dollar amount is frequently substantial, and because the funds transferred are more or less "unmarked". The reference to "unmarked" will be better explained in the next paragraph.
>
> The present invention completely abandons the concept of a locally maintained postage balance. Instead the official balance for any given user is maintained at the centralized secure computer. The balance may be increased at any time by the user through any number of secure means (e.g., a check taken to a local post office, funds mailed, or credit card transactions via the Web). All of these postage increase transactions are handled by the central secure site where standard payment verification techniques can be applied before the balance is actually updated.
>
> FIG. 6 underscores another aspect of the security offered by this invention. When funds are drawn against a license (meter) account's

> balance, contact must be made with the central secure computer and all relevant information about the mail piece must be conveyed for this transaction to be successfully processed. The information returned amalgamates the proper amount of postage and the delivery information for this particular mail piece--and it is this information that is used to create a two-dimensional IBIP barcode.

While the above passage discusses the need for security in the transaction between the postage meter vendor and the end user, there is no disclosure, teaching or suggestion of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Whitehouse is directed to a system for the electronic distribution of postage wherein all secure processing required for generating postal indicia is performed at secure central computers, not at end user computers, thereby removing the need for specialized secure computational equipment at end user sites. In Whitehouse, a typical secure central computer includes a data processor and a database of information concerning user accounts of users authorized to request postal indicia from the secure central computer. A request validation procedure authenticates received postage request with respect to the user account information in the database. A postal indicia creation procedure applies a secret encryption key to information in each authenticated postage request so as to generate a digital signature and combines the information in each authenticated postage request with the corresponding generated digital signature so as to generate a digital postage indicium in accordance with a predefined postage indicium data format. A communication procedure securely transmits the generated digital postage indicium to the requesting end user computer. (Col. 6, lines 20-45).

In Whitehouse, the data stored by the secure central computer 102 in its customer database for each meter/user account includes various information related to the account. In addition, for each meter or account, at least two child transaction tables are maintained in the transaction database 174. The first is a record of postage purchases, and the second transaction table records each postage indicium dispensing event. Whitehouse further indicates that storing data on the central computer offers very distinct advantages over conventional meters or the PSD, since the meter balances are stored on computer media rather than secure non-volatile meter registers. (Col. 10, line 45 to Col. 11, line 56).

Thus, although Whitehouse may store significant amounts of data at the central computer, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9. In fact, Applicants respectfully submit that Whitehouse teaches away from the present invention, since as noted above Whitehouse indicates that storing data on the central computer offers very distinct advantages over conventional meters or the PSD, since the meter balances are stored on computer media rather than secure non-volatile meter registers. Thus, the data stored in Whitehouse is not secured as is done in the present invention by signing the transaction records before storing them. Thus, there is no disclosure, teaching or suggestion in Whitehouse of signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

Although Whitehouse discusses the use of a digital signature, this signature is added to the other parts of the postage indicium and a message, including data representing the postage indicium with the digital signature, is encrypted and then the resulting message is transmitted to the requesting user. (Col. 13, line 15-50). This is not the same as signing a transaction record associated with generating the digital token and storing the signed transaction record in the storage device of the data center as is recited in claim 9.

For at least the above reasons, Applicants respectfully submit that claim 9 is allowable over the prior art of record. Claims 10-13, dependent upon claim 9, are allowable along with claim 9 and on their own merits.

Claim 14 includes limitations substantially similar to those of claim 9. For the same reasons given with respect to claim 9 above, Applicants respectfully submit that claim 14 is allowable over the prior art of record. Claims 15-18, dependent upon claim 14, are allowable along with claim 14 and on their own merits.

In view of the foregoing remarks, it is respectfully submitted that all claims of this case are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone No.: (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000